CLAIMS

We claim:

1. An anti-virus system for an electronic mail message, the system including detecting means for determining the presence of the electronic mail message; analysis and scanning detecting means for analysing and scanning the electronic mail message for tags indicating the presence of operable program code and for removing any such tags and operable program code from the electronic mail message; and application means for applying the electronic mail message, with the tags and operable program code removed, to server means.

2. An anti-virus system as claimed in claim 1, wherein the detecting means for determining the presence of the electronic mail message includes decomposition means for breaking the message into constituent bodies or message texts and attachments of the electronic message; the analysis and scanning means comprise scanning means for scanning the constituent bodies and attachments and the application means for applying the electronic mail message with the tags and operable program code removed to server means includes recomposition means for rebuilding the electronic message from the constituent bodies and attachments.

3. An anti-virus system as claimed in claim 1, wherein the analysis and scanning means comprise scanning means for scanning the message for predetermined character strings.

4. An anti-virus system as claimed in claim 1, wherein the application means for applying the electronic mail message with the tags and operable program code removed to server means includes replacement means for replacing the removed tag and operable program code with alternative text.

5. An anti-virus system as claimed in claim 4, wherein the replacement means is adapted to replace with alternative text for informing a recipient of the message that operable program code has been removed.

6. An anti-virus system as claimed in claim 2, wherein the analysis and scanning means include scanning means for scanning attachments for operable macros.

7. An anti-virus system as claimed in claim 2, wherein the system further comprises quarantine means for quarantining a constituent body containing operable program code and/or removing from the message and quarantining an attachment containing a macro or operable program code.

8. An anti-virus system as claimed in claim 7, wherein the quarantine means includes means for removing a macro from an attachment, quarantining the macro and releasing the attachment with the macro removed.

9. An anti-virus system as claimed in claim 7, wherein the quarantine means includes means for storing the constituent body, attachment or macro in a quarantine storage location as a quarantined item; receiving means for receiving a input indicating a decision whether the quarantined item may be delivered to an intended recipient; and dependant on the decision input either releasing the quarantined item for delivery to the intended recipient with or without the operable code removed or deleting the quarantined item.

10. An anti-virus system as claimed in claim 7, wherein the quarantine means includes informing means, on deleting the quarantined item, for informing the intended recipient and/or a sender of the message that the quarantined item has been deleted without being delivered to the intended recipient.

11. An anti-virus system as claimed in claim 6, wherein the scanning means for scanning attachments for operable macros comprises means for sequentially scanning the attachments for a plurality of predetermined character strings.

12. An anti-virus system as claimed in claim 11, wherein the means for scanning attachments for a plurality of predetermined character strings includes termination means for terminating scanning when one of the predetermined strings is not found on completely scanning the attachment.

13. An anti-virus system as claimed in claim 1, wherein the detecting means for determining the presence of the electronic mail message is adapted to capture electronic mail messages passing between a first network and a second network.

14. An anti-virus system as claimed in claim 13, wherein the detecting means for determining the presence of the electronic mail message is adapted to capture electronic mail messages passing between an internal or private network and an external or public network.

15. A method for removing a virus from an electronic mail message including the steps of (a) capturing the message; (b) scanning the message for tags indicating the presence of operable program code; (c) removing the tags and operable program code from the electronic mail message; and (d) releasing the electronic mail message with the tags and operable program code removed.

16. A method as claimed in claim 15, wherein step (c) comprises quarantining a message or a part of a message containing operable program code.

17. A method as claimed in claim 15, wherein step (a) includes the step of breaking the message into constituent bodies or message texts and attachments of the electronic message; step (b) comprises scanning the constituent bodies and attachments and step (d) includes the step of rebuilding the electronic message from the constituent bodies and attachments

18. A method as claimed in claim 15, wherein step (b) comprises scanning the message for predetermined character strings.

19. A method as claimed in claim 15, wherein step (c) includes replacing the removed tag and operable program code with alternative text.

20. A method a claimed in claim 19, wherein the step of replacing the removed tag and operable code with alternative text comprises using alternative text for informing a recipient of the message that operable program code has been removed.

21. A method as claimed in claim 17, wherein step (b) includes scanning attachments for operable macros and step (c) comprises removing from the message and quarantining any macros and/or any attachments containing macros.

22. A method as claimed in claim 16, wherein the step of quarantining a message or a part of a message comprises the steps of: storing a constituent body, attachment or macro of the message in a quarantine storage location as a quarantined item; receiving a decision whether the quarantined item may be delivered to an intended recipient; and dependant on the decision either releasing the quarantined item for delivery, with or without the operable code or macro deleted, to the intended recipient or deleting the quarantined item.

23. A method as claimed in claim 22, wherein the step of deleting the quarantined item includes informing the intended recipient and/or a sender of the message that the quarantined item has been deleted without being delivered to the intended recipient.

24. A method as claimed in claims 21, wherein the step of scanning attachments for operable macros includes sequentially scanning the attachments for a plurality of predetermined character strings.

25. A method as claimed in claim 24, wherein the step of scanning attachments for a plurality of predetermined character strings is terminated when one of the predetermined strings is not found on completely scanning the attachment.

26. A method as claimed in claim 15, wherein step (a) comprises capturing electronic mail messages passing between a first network and a second network.

27. A method as claimed in claim 26, wherein step (a) comprises capturing electronic mail messages passing between an internal or private network and an external or public network.

28. A computer program comprising code means for performing all the steps of the method of any of claims 15 to 27 when the program is run on one or more computers.

29. A computer program as claimed in claim 28, wherein the computer program is embodied on a computer-readable medium.

30. A computer program product comprising program code means stored in a computer-readable medium for performing the method of any of claims 15 to 27 when that program product is run on one or more computers.